ESD-TDR-64-581

Group Report

1964-70

E. Weiss

An Approach to Giant-Stepping

23 November 1964

Prepared under Electronic Systems Division Contract AF 19(628)-500 by

Lincoln Laboratory
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Lexington, Massachusetts

The work reported in this document was performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology, with the support of the U.S. Air Force under Contract AF 19(628)-500.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LINCOLN LABORATORY

AN APPROACH TO GIANT-STEPPING

E. WEISS

Group 66

GROUP REPORT 1964-70

23 NOVEMBER 1964

LEXINGTON MASSACHUSETTS

ABSTRACT

In certain situations there is a need for a binary sequence with extremely long period (to be measured in years, say) with equi-distribution of zero and ones (and for pairs, triples, etc. insofar as possible) and having an additional property which may be called giant-stepping. We shall describe one procedure for handling this problem; our approach is based on the assumption that it is neither feasible nor desirable to set up way stations (whether pre-programmed or not) along the way.

Accepted for the Air Force
Stanley J. Wisniewski
Lt Colonel, USAF
Chief, Lincoln Laboratory Office

An Approach to Giant-Stepping

In certain situations there is a need for a binary sequence with extremely long period (to be measured in years, say) with equi-distribution of zero and ones (and for pairs, triples, etc. insofar as possible) and having an additional property which may be called giant-stepping. By this term we have the following in mind. Suppose that we have two identical machines which begin to turn out our sequence in a synchronous fashion at time t_o—and that at some later time one of them breaks down for an indefinite period. When this machine is repaired, one wants to return quickly to synchronous production of the sequence—that is, a giant-step is required in order to catch up with the sequence as produced by the functioning machine. There are other ways of formulating the giant-stepping requirement, but they are all equivalent. The important thing is that the catching up process should be a matter of a few minutes, no matter how long the breakdown period (days, weeks, or even months).

We shall describe one procedure for handling this problem; our approach is based on the assumption that it is neither feasible nor desirable to set up way stations (whether pre-programmed or not) along the way.

Before giving proofs of the assertions on which our solution depends, it is useful to make some remarks about notation and terminology. If m and n are positive integers then (m, n) denotes the greatest common

divisor of m and n; this is the unique positive integer which divides both m and n and is divisible by every other common divisor of m and n. The least common multiple of m and n will be denoted by [m, n]. Suppose that a and n are positive integers then by the order of a mod n is meant the smallest integer t such that $a^t = 1 \pmod{n}$; if s is such that $a^s = 1 \pmod{n}$ then $t \mid s$.

Now consider an infinite binary sequence $A = (a_1, a_2, \ldots,)$. We say that A has $n \geq 1$ as a period when

$$a_{i+n} = a_i \qquad i = 1, 2, \ldots$$

There is a unique smallest period of A—called the period of A—it is the greatest common divisor of all the periods of A. If $B = (b_1, b_2, \ldots)$ is another infinite binary sequence, then by A + B we mean the binary sequence whose i^{th} term is $a_i + b_i$ for all $i = 1, 2, \ldots$. We shall also need some of the standard facts about maximal length shift register sequences; proofs of them are rather plentiful in the literature—see, for example, [3] or [4]. With these preliminaries out of the way, let us turn to the facts upon which our technique is based.

Fact 1. Let n_1, n_2 be positive integers; then

$$(n_1, n_2) = 1 \Leftrightarrow (2^{n_1} - 1,\ 2^{n_2} - 1) = 1$$

Proof. Suppose that $(n_1, n_2) = d > 1$, and write $n_1 = r_1 d$, $n_2 = r_2 d$. Therefore, $2^{n_1} - 1 = (2^d)^{r_1} - 1$ and $2^{n_2} - 1 = (2^d)^{r_2} - 1$

Since for any positive integer s we have

$$x^s - 1 = (x - 1)(x^{s-1} + x^{s-2} + \cdots + x + 1)$$

it follows that $2^d - 1$ (which is > 1) divides both $2^{n_1} - 1$ and $2^{n_2} - 1$—so $(2^{n_1} - 1, 2^{n_2} - 1) \neq 1$.

Conversely, suppose that $(n_1, n_2) = 1$. If $(2^{n_1} - 1, 2^{n_2} - 1) = d > 1$ then let p be a prime (which must be odd) that divides d. Thus, $p \mid (2^{n_1} - 1)$, $p \mid (2^{n_2} - 1)$ and we may write

$$2^{n_1} = (\text{mod } p) \qquad 2^{n_2} = 1 \ (\text{mod } p)$$

Let n be the order (see [2]) of $2 (\text{mod } p)$—that is, n is the order of 2 in the multiplicative group of the field with p elements. Of course, $n > 1$. The congruences imply that $n \mid n_1$ and $n \mid n_2$; hence, $n \mid (n_1, n_2) = 1$, a contradiction. This completes the proof.

Fact 2. Let $A_1 = (a_1^{(1)}, a_2^{(1)}, \ldots)$ be a sequence of period m_1, and let $A_2 = (a_1^{(2)}, a_2^{(2)}, \ldots)$ be a sequence of period m_2; then $[m_1, m_2]$ is a period of $A_1 + A_2$. Furthermore, if $(m_1, m_2) = 1$ then the period of $A_1 + A_2$ is $[m_1, m_2] = m_1 m_2$

Proof. By hypothesis, we know that for $k_1 = \dfrac{[m_1, m_2]}{m_1}$ and all i, we have

$$a_i^{(1)} = a_{i+m_1}^{(1)} = a_{i+k_1 m_1}^{(1)}$$

In the same way, for $k_2 = \dfrac{[m_1, m_2]}{m_2}$ and all i, we have

$$a_i^{(2)} = a_{i+m_2}^{(2)} = a_{i+k_2 m_2}^{(2)}$$

Since $k_1 m_1 = k_2 m_2$ it follows that for all i

$$a_i^{(1)} + a_i^{(2)} = a_{i+[m_1, m_2]}^{(1)} + a_{i+[m_1, m_2]}^{(2)}$$

which says that $[m_1, m_2]$ is a period of $A_1 + A_2$.

Suppose that $[m_1, m_2]$ is not the period of $A_1 + A_2$, and let c denote the period—so $c \mid [m_1, m_2]$, $c \neq [m_1, m_2]$. Then there exists a positive integer m with the properties:

$$c \mid m, \quad m \mid [m_1, m_2], \quad \frac{[m_1, m_2]}{m} = p, \quad p \text{ prime}$$

In particular, m is a period of $A_1 + A_2$. If $(m_1, m_2) = 1$ then exactly one of m_1, m_2 divides m—let it be m_1. Then, A_1 and $A_1 + A_2$ both have m as a period; hence so does $A_1 + (A_1 + A_2) = A_2$. This contradicts $m_2 \nmid m$, so that $m_1 m_2$ is the period, and the proof is complete.

Fact 3. In one period of a maximal length shift register sequence arising from a primitive polynomial of degree n, every k-tuple (for each $k = 1, \ldots, n$) occurs equally often—namely, 2^{n-k} times—except for the all zero k-tuple which occurs $2^{n-k} - 1$ times.

Proof. Let $A = (a_1, a_2, \ldots)$ be the sequence in question. Since it is a linear recursive sequence arising from a primitive polynomial of degree n, its period is $m = 2^n - 1$—so $a_{i+m} = a_i$ for $i = 1, 2, \ldots$. Now, fix k. We must examine the k-tuples

$$(a_j, a_{j+1}, \ldots, a_{j+k-1}) \qquad j = 1, \ldots, m$$

and count the number of times that an arbitrary k-tuple of zeros and ones appears. We recall that, because A is a maximal length shift register sequence, the n-tuples

$$A^{(j)} = (a_j, a_{j+1}, \ldots, a_{j+n-1}) \qquad j = 1, \ldots, m$$

are all distinct and $\neq (0, \ldots, 0)$. In other words, if V_n denotes the set of all n-tuples of zeros and ones, and V'_n denotes V_n with the all zero n-tuple excluded, then

$$\{A^{(j)} \mid j = 1, \ldots, m\} = V'_n$$

Thus we are concerned with the k-tuples consisting of the first k coordinates of the elements of V'_n. It follows immediately that any non-zero k-tuple occurs 2^{n-k} times, and that the zero k-tuple occurs $2^{n-k} - 1$ times. This completes the proof.

Fact 4. Let $n_1 < n_2 < \ldots < n_r$ be positive integers that are relatively prime in pairs, and let $A_1, \ldots, A_r$ denote maximal length shift register

sequences of periods $m_i = 2^{n_i} - 1$, $i = 1, \ldots, r$. Then in one period of the sequence $A = \sum_1^r A_i$ (whose period is $\prod_1^r m_i$) every k-tuple (for each $k = 1, \ldots, n_1$) occurs equally often—namely

$$\varphi = \frac{\prod_1^r m_i + (-1)^{r+1}}{2^k} \quad \text{times}$$

except for the all zero k-tuple which occurs $\varphi + (-1)^r$ times.

Proof. The case $r = 1$ has already been done. The proof is by induction on r, but because the notation becomes extremely cumbersome, we shall deal only with the case $r = 2$. This will suffice to indicate how the proof goes in general.

Fix any $k \leq n_1$, and let $D = (d_1, \ldots, d_k)$ denote an arbitrary k-tuple $\neq (0, \ldots, 0)$. We must count the number of times D appears in one period (of length $m_1 m_2$) of $A_1 + A_2$. First of all, we note that D can be written in the form $D = B + C$ where $B = (b_1, \ldots, b_k)$ and $C = (c_1, \ldots, c_k)$ are both $\neq (0, \ldots, 0)$ in exactly $2^k - 2$ ways; in fact, making a choice of B determines C. Now the k-tuple B appears exactly $2^{n_1 - k}$ times in a single period of A_1—denote them by $B_1, \ldots, B_{2^{n_1 - k}}$; and the k-tuple C appears exactly $2^{n_2 - k}$ times in a single period of A_2—denote them by $C_1, \ldots, C_{2^{n_2 - k}}$. Because m_1 and m_2 are relatively prime each sum

$$B_i + C_j \qquad i = 1,\ldots, 2^{n_1-k} \qquad j = 1,\ldots, 2^{n_2-k}$$

appears exactly once in a period of $A_1 + A_2$. Thus, from a single such pair B, C we get D in a period of $A_1 + A_2$ exactly $(2^{n_1-k})(2^{n_2-k})$ times—so that running over all such pairs B, C we see that

$$D \text{ appears } (2^{n_1-k})(2^{n_2-k})(2^k - 2) \text{ times}$$

We must also count the appearances of $D = B + C$ where $B = (0,\ldots, 0), C = D$. Here, B appears $2^{n_1-k} - 1$ times in a period of A_1, while C appears 2^{n_2-k} times in a period of A_2. It follows that from this pair, B, C

$$D \text{ appears } (2^{n_1-k} - 1)(2^{n_2-k}) \text{ times}$$

Finally, we may write $D = B + C$, $C = (0,\ldots, 0)$, $B = D$, and from this pair

$$D \text{ appears } (2^{n_1-k})(2^{n_2-k}) \text{ times}$$

These 3 ways provide all appearances of D in a period of $A_1 + A_2$—the number of appearances is then

$$(2^{n_1-k})(2^{n_2-k})(2^k-2) + (2^{n_1-k}-1)(2^{n_2-k}) + (2^{n_1-k})(2^{n_2-k}-1)$$

$$= \frac{(2^{n_1}-1)(2^{n_2}-1) + (-1)^3}{2^k} = \frac{m_1 m_2 + (-1)^3}{2^k}$$

which is the desired result.

It remains to count the appearances of $D = (0,\ldots,0)$ in a period of $A_1 + A_2$. By the techniques used above, we see that $(0,\ldots,0)$ appears

$$(2^{n_1-k})(2^{n_2-k})(2^k-1) + (2^{n_1-k}-1)(2^{n_2-k}-1)$$

$$= \frac{2^{n_1+n_2} - 2^{n_1} - 2^{n_2} + 2^k}{2^k} = \frac{m_1 m_2 - 1}{2^k} + (-1)^2$$

times. This completes our sketch of the proof.

From all this it follows that a solution to our problem is given by simply adding mod 2 the outputs of several shift registers associated with primitive polynomials. Let us illustrate this with a concrete example. Suppose that the desired sequence is to run at the rate of 10^6 bits per second with period on the order of 100 years. The number of bits in 100 years is then approximately

$$(10^6)(60)(60)(24)(365)(100) < (2^{20})(2^6)(2^6)(2^5)(2^9)(2^7) = 2^{53}$$

Consider the primitive polynomials

$$f_1(x) = x^{17} + x^3 + 1$$

$$f_2(x) = x^{19} + x^5 + x^2 + x + 1$$

$$f_3(x) = x^{21} + x^2 + 1$$

of degrees $n_1 = 17$, $n_2 = 19$, $n_3 = 21$. Let A_1, A_2, A_3 denote the maximum length shift register sequences they determine. Then $A = A_1 + A_2 + A_3$ has period $(2^{17}-1)(2^{19}-1)(2^{21}-1) > 2^{53}$—that is, greater than 100 years. Suppose that at any time we wish to enter the sequence A at the $r^{\underline{th}}$ bit, $1 \leq r < (2^{17}-1)(2^{19}-1)(2^{21}-1)$. Let r_i $i = 1, 2, 3$ be the remainder upon division of r by $m_i = 2^{n_i}-1$; so $0 \leq r_1 < 131,071$, $0 \leq r_2 < 524,287$, $0 \leq r_3 < 2,097,151$. Now, run the i^{th} shift register, starting from its initial setting, until it reaches the $r_i^{\underline{th}}$ bit. This takes on the order of 2 seconds!!! Upon reaching the $r_i^{\underline{th}}$ bit the shift register stops until all three are ready to proceed simultaneously from the required place. In particular, giant-stepping is quite feasible. Of course, the zeros and ones of our sequence are nicely distributed, and so are blocks of terms of length upto and including 17. It should also be noted that, in view of our example, the clock or timing device which serves to keep count of the bits should be set up in terms of several cyclic devices of periods $m_i = 2^{n_i}-1$—in other words, counting is to be done modulo the various m_i, rather than in the scale of 10.

REFERENCES

1. G. Birkhoff and S. MacLane, A Survey of Modern Algebra, Macmillan, New York (1944).

2. W. J. LeVeque, Topics in Number Theory, 1, Addison-Wesley (1956).

3. W. W. Peterson, Error-Correcting Codes, MIT Press (1961).

4. E. Weiss, "Some Connections between Linear Recursive Sequences and Error-Correcting Codes: Informal Lectures, Group Report 55-22.

DISTRIBUTION

Group 28

C. R. Arnold

Division 6

G. P. Dinneen
W. E. Morrow, Jr.

Group 62

P. R. Drouilhet
B. Gold
K. L. Jordan, Jr.
I. L. Lebow
P. Rosen

Group 63

J. Max
W. G. Schmidt
H. Sherman

Group 64

P. Green
R. Price

Group 66

F. Belvin
R. G. Enticknap
T. J. Goblick, Jr.
J. R. Kinney
T. S. Pitcher
R. T. Prosser
B. Reiffen
E. Weiss
H. Yudkin
File (10)

Security Classification

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*

Lincoln Labs.,
Lexington, Mass.

2a. REPORT SECURITY CLASSIFICATION

UNCLASSIFIED

2b. GROUP

N/A

3. REPORT TITLE

An Approach to Giant-Stepping

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

Group Report

5. AUTHOR(S) *(Last name, first name, initial)*

Weiss, E.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
Nov 64	13	4

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
AF19(628)500	GR-1964-70
b. PROJECT NO.	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	ESD-TDR-64-581

10. AVAILABILITY/LIMITATION NOTICES

Qualified Requesters May Obtain from DDC.
Aval from OTS.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	ESD, L.G. Hanscom Field, Bedford, Mass.

13. ABSTRACT

In certain situations there is a need for a binary sequence with extremely long period (to be measured in years, say) with equi-distribution of zero and ones (and for pairs, triples, atc. insofar as possible) and having an additional property which may be called giant-stepping. We shall describe one procedure for handling this problem; our approach is based on the assumption that it is neither feasible nor desirable to set up way stations (whether pre-programmed or not) along the way.

DD FORM 1 JAN 64 1473

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Mathematics Algebra Number Theory Error Correcting Codes Binary Sequence						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization *(corporate author)* issuing the report.

2*a*. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2*b*. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7*a*. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7*b*. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8*a*. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8*b*, 8*c*, & 8*d*. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9*a*. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9*b*. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers *(either by the originator or by the sponsor)*, also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through

_____."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through

_____."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through

_____."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring *(paying for)* the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as *(TS)*, *(S)*, *(C)*, or *(U)*.

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, rules, and weights is optional.